



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/959,575	10/28/97	CARLSON	R 1505/5A

STUART T. LANGLEY
DORR CARSON SLOAN & PETERSON
3010 E. 6TH AVENUE
DENVER CO 80206

LM01/1027

EXAMINER

MEISLAHN, D

ART UNIT	PAPER NUMBER
2767	7

DATE MAILED: 10/27/99

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No. 08/959,575	Applicant(s) Carlson
Examiner Douglas Meislahn	Group Art Unit 2767

Responsive to communication(s) filed on Sep 29, 1999

This action is FINAL.

Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire 3 month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

Claim(s) 17-22 and 29-43 is/are pending in the application.

Of the above, claim(s) _____ is/are withdrawn from consideration.

Claim(s) _____ is/are allowed.

Claim(s) 17-22 and 29-43 is/are rejected.

Claim(s) _____ is/are objected to.

Claims _____ are subject to restriction or election requirement.

Application Papers

See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

The drawing(s) filed on _____ is/are objected to by the Examiner.

The proposed drawing correction, filed on _____ is approved disapproved.

The specification is objected to by the Examiner.

The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

All Some* None of the CERTIFIED copies of the priority documents have been

received.

received in Application No. (Series Code/Serial Number) _____.

received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____

Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

Notice of References Cited, PTO-892

Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

Interview Summary, PTO-413

Notice of Draftsperson's Patent Drawing Review, PTO-948

Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

Art Unit: 2767

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 29 September 1999 which amended the title and claims 17, 33, 39, 40, 42, and 43. The amendment to the title has overcome the objection.

Response to Arguments

2. Applicant's arguments filed 29 September 1999 have been fully considered but they are not persuasive.

In response to applicant's argument that Vasseur I checks only the key generation and not the random number generation, the examiner notes that computers use binary logic which is a number based system.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., infinite number length, encryption circuit used to randomize numbers) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Art Unit: 2767

Applicant's argument that Vasseur I does not show a continuous stream of numbers because he has a shut-off for statistically unverified random numbers is moot because applicant's claims are directed only to statistically verified random numbers.

DMS
10-25-91

Vasseur I's invention is a system for checking the ~~r~~andom character or sequences. A checker, or, as applicant says, verifier, is inherent.

In order to check the randomness of numbers, the numbers must be checked against each other, which requires storage. As applicant has repeated in his arguments, Vasseur I is directed to a key generator. Key generators distribute the keys that they generate so that the keys can be used.

In response to applicant's argument that Murata is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, both Murata et al. and Vasseur I use memories to store data.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5

Art Unit: 2767

USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir.

1992). In this case, the benefits of Murata et al.'s buffer are universally desirable.

Vasseur II shows two generators that produce pseudo-random sequences. Vasseur I has taught a controller that connects to random number generators and continuously provides a series of statistically verified pseudo-random numbers.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Vasseur II can be used to aid in assuring the randomness of the random numbers generated in Vasseur I. As applicant has noted, Vasseur I stops running when non-random numbers are detected.

The examiner will address applicant's challenges to the Official Notices when the challenges are done properly.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

Art Unit: 2767

A person shall be entitled to a patent unless --

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 17, 30, 33, 34, and 43 are rejected under 35 U.S.C. 102(b) as being anticipated by Vasseur (3309509).

Vasseur's invention, a system for checking the random characteristics of sequences of N symbols, clearly anticipates the verifier of applicant's invention. Figure 2 shows the operation of a key generator which, like the at least one random number circuit of the present invention, produces random numbers. Although not expressly stated in Vasseur, the storage and controlled distribution of keys is inherent to key generation, and this corresponds to applicant's controller that stores the pseudo-random numbers.

In figure 2, element c is a decoder, which can be used in an encryption circuit.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 18 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vasseur (3309509) in view of Murata et al. (5361323).

Art Unit: 2767

Vasseur teaches a random number generation and verification circuit. He does not talk about a buffer storing numbers. In lines 16-18 of column 18, Murata et al. talk about outputting pseudo-random numbers that have been stored in a buffer. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to store the verified random numbers of Vasseur in a buffer as taught by Murata et al. This would provide a repository of values that could be used immediately as opposed to generating values, which takes time, as needed.

7. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vasseur (3309509) in view of Vasseur (4179663).

Vasseur (3309509) teaches a random number generation and verification circuit. He does not disclose in this patent using two random number generators. In Vasseur (4179663), a system using two sequence generators is taught. Figure 1 shows these two generators as elements 11 and 14. From line 46 of column 2 through line 24 of column 3, Vasseur (4179663) shows how these tandem generators can be used to minimize non-randomness. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use two sequence generators to produce random numbers and thereby increase the probabilities of the produced numbers being random.

8. Claims 19 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vasseur (3309509).

Art Unit: 2767

Vasseur teaches a random number generation and verification circuit. He does not say that the random number generator is an ANSI X9.17. Official notice is taken that ANSI X9.17 circuits are old and well-known. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use the ANSI X9.17, the industry standard, circuit to generate the random numbers in Vasseur's invention in order to increase compatibility.

9. Claims 21 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vasseur (3309509) in view of Murata et al. (5361323) as applied to claims 18 and 36 above.

Vasseur in view of Murata et al. teaches a random number generation and verification circuit which stores its outputs in a buffer. They do not say that the buffer uses a FIFO system. Official notice is taken that FIFO systems are old and well-known. A FIFO system would maintain the random nature of the numbers. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement a FIFO system in the output of numbers from the circuit of Vasseur in view of Murata et al, thus maintaining randomness.

10. Claims 22, 38, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vasseur (3309509) in view of Murata et al. (5361323) as applied to claims 18 and 36 above.

Vasseur in view of Murata et al. teaches a random number generation and verification circuit which stores its outputs in a buffer. They do not disclose that the buffer outputs numbers at a lesser rate than it receives numbers, nor that the buffer can, for short periods of time, output numbers faster than it receives numbers. Official notice is taken that it is old and well-known that

Art Unit: 2767

a data storage circuit must receive inputs at a rate greater than or equal to the rate of outputs. Otherwise, the circuit could be unable to output data fast enough. Official notice is also taken that it is old and well-known to allow for data output at a rate faster than data input for a short period of time. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to input values to the buffer at a rate such that the buffer would never run out of values to output. This would be accomplished by inputting values at a greater rate than they were output. It would also have been obvious to a person of ordinary skill in the art at the time the invention was made to allow the buffer to output values at a rate greater than values are input for short time periods, thereby allowing for faster operations over the short time period. Also, by outputting these values at an increased rate, memory space would be freed in the buffer.

11. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vasseur (3309509).

Vasseur teaches a random number generation and verification circuit. He does not say that the verification circuits use an algorithm selected from the set of a Runs Test, a K-S test, a Chi-square test and a serial test. Official notice is taken that the Runs Test, K-S test, Chi-square test, and serial test are old and well-known as tests to check for randomness. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ one of the set of the Runs Test, K-S test, Chi-square test, and serial test to measure randomness. As applicant has provided no reason for one or any of the tests being superior to the

Art Unit: 2767

rest, the examiner sees no reason to explain why these tests are specifically obvious other than that they are old and well-known.

12. Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vasseur (3309509).

Vasseur teaches a random number generation and verification circuit. He does not display an encryption circuit between the random number generation circuit and the controller. Official notice is taken that encryption circuits can take otherwise non-random series and, through encryption, make the series random. Also, official notice is taken that encryption of values secures the values from illicit viewers. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt the outputs of the random number generator to assure their randomness and to make them unreadable to an outside party.

13. Claims 31 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vasseur (3309509).

Vasseur teaches a random number generation and verification circuit. He says nothing about using DES circuits to process the random numbers. Official notice is taken that DES circuits are old and well-known and can be used to randomize data and to secure data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use the DES to encrypt the outputs of the random number generator to assure their randomness and to make them unreadable to an outside party.

Art Unit: 2767

14. Claims 32 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vasseur as applied to claims 30 and 39 above.

Vasseur teaches a random number generation and verification circuit where the outputs of the random number generator are encrypted. He does not say that the encryption uses IDEA encryption. Official notice is taken that IDEA is old and well-known in the art of encryption. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use IDEA, as a well-known algorithm, to encrypt data.

Conclusion

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 2767

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached Monday-Thursday and every other Friday from 8:30 AM to 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod Swann, can be reached at (703) 308-7791.

The fax number for Formal or Official faxes to Technology Center 2700 is (703) 308-9051 or 9052. Draft or Informal faxes for this Art Unit can be submitted to (703) 305-0040.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.



DJM
October 25, 1999



TOD R. SWANN
SUPERVISORY PATENT EXAMINER